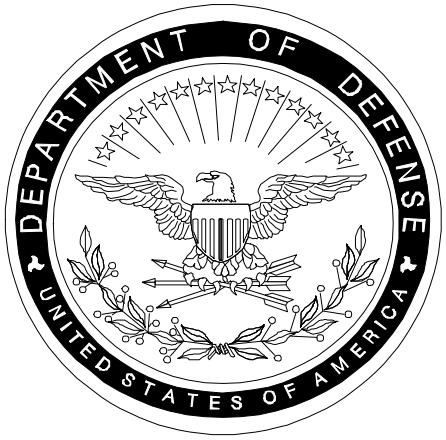
NOT MEASUREMENT SENSITIVE

MIL-STD-2045-18500-5
28 October 1993

MILITARY STANDARD

Information Technology
DoD Standardized Profiles AMHXn(D)
Message Handling Systems
Message Security Protocol
(MSP)

Part 5: AMHx4(D) - MSP Requirements for MS Access (P7)



AMSC N/A

AREA DCPS

Foreword

This military standard is approved for use by all Departments and Agencies of the Department of Defense (DoD).

Beneficial comments (recommendations, additions, deletions) and any pertinent data that may be of use in improving this Mil-Std should be addressed to the:

Joint Interoperability and Engineering Organization (JIEO)
ATTN: TBBD
Building 286
Fort Monmouth, New Jersey 07703-5613

by using the Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this Mil-Std or by memorandum.

This DoD Standardized Profile (DSP) is a functional standard produced by the (DTMP) Working Group 3 on Security. DTMP functional standards are functional groupings of base standards. Referenced base standards may be commercial, DoD or de facto standards, although International Standards (produced by ISO, CCITT, and other bodies) are preferred when possible.

This part of MIL-STD 2045-18500 contains two normative annexes.

This document forms part of a DoD Standardized Profile (DSP) for Message Security Protocol (MSP) covering Message Security requirements, AMHx4(D), for DoD. It is outside of the current Taxonomy and Framework for International Standardized Profiles. It will correspond to the DoD extensions to that taxonomy found in MIL-HDBK-829. This DSP is a content-specific profile for the MSP content type as defined in SDN.701.

The current technical content of the document has been derived wherever possible from the Secure Data Network System (SDNS) MSP specification SDN.701.

The Preparing Activity for this standard is the Data Communication Protocol Standards Technical Management Panel (DTMP). The custodians for the document are identified in the Defense Standardization Program, "Standardization Directory (SD-1)" and are classified in the Federal Supply Classification (FSC) system under Data Communication Protocol Standards (DCPS). Additional information can be obtained from:

Joint Interoperability and Engineering Organization
ATTN: DTMP Chairman
Building 286
Ft. Monmouth, New Jersey 07703-5613

Contents

Annexes

Figure

Table

Introduction

This DoD Standardized Profile (DSP) is defined within the context of functional standardization, in accordance with the principles specified by ISO/IEC TR 10000, “Framework and Taxonomy of International Standardized Profiles,” and MIL-HDBK-829. The context of functional standardization is one part of the overall Information Technology (IT) standardization activities, covering base standards, profiles, and registration mechanisms. A profile defines a combination of base standards that collectively perform a specific, well-defined IT function. Profiles standardize the use of options and other variations in the base standards to promote system interoperability and provide a basis for developing uniform, internationally recognized system tests.

One of the most important roles for a DSP is to serve as the basis for development of recognized tests. DSPs also guide implementors in developing systems that fit the needs of the U.S. Department of Defense (DoD). DSPs are produced not simply to ‘legitimize’ a particular choice of base standards and options, but to promote real system interoperability. The development and widespread acceptance of tests based on this and other DSPs is crucial to successful realization of this goal.

This part of MIL-STD 2045-18500 covers access to a Message Store (MS) using the P7 MS Access Protocol to support an MSP environment. It specifies any additional P7 support to that specified in AMH1n(D) and defines conformance requirements for an MS that supports remote access for MSP use, and for a remote MS-user in a MSP context (MSP UA), with respect to support of P7 and associated functionality (requiring conformance to AMH13(D) and by reference to the common MSP specifications in Part 1).

This part of MIL-STD 2045-18500 contains two normative annexes:

Annex A DSP Requirements List

Annex B Amendments and corrigenda

Information technology - Defense Standardized Profiles AMHx4(D) - Message Handling Systems - Message Security Protocol

Part 5 : AMHx4(D) MSP Requirements for MS Access (P7)

1 Scope

1.1 General

This part of MIL-STD 2045-18500 covers access to a Message Store (MS) in an MSP environment using the P7 MS Access Protocol (see also figure 1). These specifications are part of the Message Security Protocol application functions, as described in MIL-STD 2045-18500, and are based on the Common DoD Messaging content type-independent specifications in MIL-STD 2045-17501.

1.2 Position within the taxonomy

This part of MIL-STD 2045-18500, AMHxn(D) is the fifth of five parts of a DSP for Message Handling Systems - Message Security. The DSP consists of the following:

Part 1 - Message Security (MSP) Service Support

Part 2 - AMHx1(D) - MSP Content Protocol

Part 3 - AMHx2(D) - MSP Requirements for Message Transfer (P1)

Part 4 - AMHx3(D) - MSP Requirements for MTS Access (P3)

Part 5 - AMHx4(D) - MSP Requirements for MS Access (P7)

This DSP must be combined with the DSP called “AMH1(D), Message Handling Systems - Common DoD Messaging” (see also ISO/IEC TR 10000-1, 8.2 for the definition of multipart ISPs).

The AMH1(D) DSP consists of the following:

Part 1 - MHS Service Support

Part 2 - Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for Use by DoD MHS

Part 3 - AMH11(D) - Message Transfer (P1)

Part 4 - AMH12(D) - MTS Access (P3)

Part 5 - AMH13(D) - MS Access (P7)

It may be combined with any DoD approved T-Profile (see ISO/IEC TR 10000) specifying the OSI connection-mode Transport service.

1.3 Scenario

The model shown in Figure 1 depicts an MSP user accessing a MSP message store (MS), specifically, the interconnection between an MS and an MS-user (a MSP user agent) using the P7 protocol, as shown in figure 1.
The AMHx4(D) covers all aspects of the MS Abstract Service as defined in ISO/IEC 10021-5, when realized using the P7 protocol in an MSP environment.

2 Normative references

The following documents contain provisions which, through reference in this text, constitute provisions of this part of MIL-STD 2045-18500. At the time of publication, the editions indicated were valid. All documents are subject to revision, and parties to agreements based on this part of MIL-STD 2045-18500 are warned against automatically applying more recent editions of the documents listed below, since the references made by DSPs to such documents may be specific to a particular edition. Members of IEC and ISO maintain registers of currently valid International Standards and ISPs, and CCITT maintains published editions of its current Recommendations.

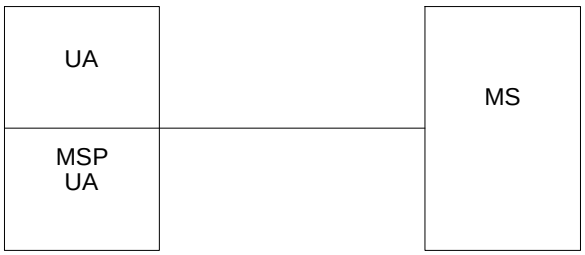


Figure 1 - **AMHx4(D) scenario**

Amendments and corrigenda to the base standards referenced are listed in annex B.

NOTE - References in this part of MIL-STD 2045-18500 to specific clauses of ISO/IEC documents shall be considered to refer also to the corresponding clauses of the equivalent CCITT Recommendations (as noted below) unless otherwise stated.

Government documents:

MIL-STD 2045-17501, *Information technology - DoD Standardized Profiles - Message Handling Systems - Common DoD Messaging -*

MIL-HDBK 829, Volumes 1 , *Mil-Std 2045 Series Documentation, 23 April 1993*

MIL-HDBK 829, Volumes 2 , *Guidelines for Data Communications Protocol Standards (DCPS) DoD Standardized Profiles (DSPs), 23 April 1993*

SDN.701: *Message Security Protocol, Revision 2.0, December 11, 1992.*

SDN.702: *SDNS Directory Specifications for Utilization with the SDNS Message Protocol, Revision 2.2, April 29, 1993.*

SDN.703: *SDNS X.400 Rekey Agent Protocol, Version 1.0, November 20, 1991.*

SDN.801: *SDNS Access Control Concept Document, Revision 1.3, July 26,1989.*

SDN.802: *SDNS Access Control Specification, July 25, 1989.*

DoD activities may obtain copies of DoD directives through their own publication channels or from the DoD Single Stock Point, Standardization Document Order Desk, 700 Robbins Avenue, Building 4D, Philadelphia, PA 19111-5094. Other federal agencies and the public may purchase copies from the U.S. Department of Commerce, National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161.

International Standards Organization (ISO)

ISO 7498-2: 1990, *Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.*

ISO/IEC 9594: 1990*, Information technology - The Directory. [see also CCITT Recommendations X.5xx(1988)]*

ISO/IEC 9594-8: 1990*, Information technology - The Directory - Part 8: Authentication framework. [see also CCITT Recommendation X.509(1988)]*

ISO/IEC TR 10000-1: 1990*, Information technology - Framework and taxonomy of International Standardized Profiles - Part 1: Framework.*

ISO/IEC TR 10000-2: 1990*, Information technology - Framework and taxonomy of International Standardized Profiles - Part 2: Taxonomy.*

ISO/IEC 10021-1: 1990, *Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 1: Service Overview. [see also CCITT Recommendation X.400(1988)]*

ISO/IEC 10021-2: 1990*, Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 2: Overall Architecture. [see also CCITT Recommendation X.402(1988)]*

ISO/IEC 10021-4: 1990*, Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 4: Message Transfer System: Abstract Service Definition and Procedures. [see also CCITT Recommendation X.411(1988)]*

ISO/IEC 10021-5: 1990*, Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 5:.Message Store: Abstract Service Definition. [see also CCITT Recommendation X.413(1988)]*

ISO/IEC 10021-6: 1990, *Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 6: Protocol Specifications. [see also CCITT Recommendation X.419(1988)]*

ISO/IEC Draft pDISP 10611:[1] September 1992, *Information technology - International Standardized Profiles AMH1n - Common Messaging*

(Application for copies of these documents should be addressed to ISO, Van Demonstrate 94, 1013 CN Amsterdam, Netherlands.)

3 Definitions

For the purposes of this part of MIL-STD 2045-18500, this section contains additional definitions that apply. Terms used in this part of MIL-STD 2045-18500 are defined in the referenced base standards.

3.1 General

Basic requirement : An Element of Service (EoS), protocol element, procedural element, or other identifiable feature specified in the base standards that must be supported by all MHS implementations conforming to this profile.

Functional group : A specification of one or more related EoS, protocol elements, procedural elements, or other identifiable features specified in the base standards which together support a significant optional area of MHS functionality.

[1] To be published.

NOTE - A functional group can cover any combination of MHS features specified in the base standards for which the effect of implementation can be determined at an external interface, i.e., via a communications protocol. Other forms of exposed interface are outside the scope of this version of MIL-STD 2045-18500.

3.2 Support classification

To specify the support level of arguments, results, and other protocol features for this part of MIL-STD 2045-18500, the following terminology is defined.

In the case of protocol elements, the classification is relative to that of the containing element, if any. If no classification is specified for the constituent elements of a non-primitive element, then they shall be considered to have the classification of that element. Where the range of values to be supported for an element is not specified, then all values defined in the DoD base standards shall be supported.

3.2.1 Static capability

To following classifications are used in this part of MIL-STD 2045-18500 to specify static conformance requirements or capability.

Mandatory full support (**m**) The element or feature shall be supported fully. An implementation shall be able to generate the element and/or receive the element, and perform all relevant associated procedures (implying the ability to handle both the syntax and semantics of the element) as specified in the DoD base standards. Where support for origination (generation) and reception are not distinguished, both capabilities shall be assumed.

Optional support (**o**) An implementation is not required to support the element. If support is claimed, the element shall be treated as if it were specified as mandatory support. If support for origination is not claimed, then the element is not generated. If support for reception is not claimed, then an implementation may ignore the element on delivery, but will not treat it as an error.

Conditional support (**c**) The element shall be supported under the conditions specified in this part of MIL-STD 2045-18500. If these conditions are met, the element shall be treated as if it were specified as mandatory support. If these conditions are not met, the element shall be treated as if it were specified as optional support, unless otherwise stated.

Out of scope (**i**) The element is outside the scope of this part of MIL-STD 2045-18500. It will not be the subject of a DSP conformance test.

Not applicable (**–**) The element does not apply in the particular context in which this classification is used.

Prohibited (**x**) The element shall not be originated by an implementation claiming conformance to this profile. If the element is received, it may be treated as a protocol violation unless otherwise stated.

3.2.2 Dynamic behavior

The above classifications are used in this part of MIL-STD 2045-18500 to specify static conformance requirements (capability); dynamic conformance requirements (behavior) are as specified in the DoD base standards. However, in a few cases it has been necessary to specify additional dynamic conformance requirements in this profile. These are specified using a second classification code for an element as follows.

Required (**r**) The element always shall be present. An implementation shall ensure that the element always is generated or otherwise used, as appropriate. If the element is absent on reception, the communication shall be terminated or rejected with an appropriate error indication as specified in the DoD base standards.

Excluded (**x**) The element never shall be present. An implementation shall ensure that the element never is generated or otherwise used, as appropriate. If the element is present on reception, the communication shall be terminated or rejected with an appropriate error indication as specified in the DoD base standards.

4 Abbreviations

ACSE	Association Control service Element
AMH	Application Message Handling
ASN.1	Abstract Syntax Notation One
AV	Auxiliary Vector

CA	Certification Authority
CCITT	International Telegraph and Telephone Consultative Committee
DIB	Directory Information Base
DoD	Department of Defense
DSA	Directory Service Agent
DSP	DOD Standardized Profile
DUA	Directory User Agent
EMS	Express Mail Service
EoS	Element of Service
FG	Functional Group
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ISP	International Standardized Profile
KMS	Key Management System
LMA	Local Management Authority
LRBAC	Local Rule-Based Access Control
MHS	Message Handling Systems
ML	Mail List
MLA	Mail List Agent
MOTIS	Message-Oriented Text Interchange Systems
MS	Message Store
MSP	Message Security Protocol
MSP UA	Message Security Protocol User Agent
MT	Message Transfer
MTA	Message Transfer Agent
MTS	Message Transfer System
OSI	Open Systems Interconnection
PICS	Protocol Implementation Conformance Statement
PRBAC	Partition Rule-Based Access Control
QoS	Quality of Service
ROSE	Remote Operation Service Element
RTSE	Reliable Transfer Service Element
SDNS	Secure Data Network System
UA	User Agent
UKM	User Keying Material

Support level for protocol elements and features (see 3.2):

m	mandatory full support
o	optional support
c	conditional support
i	out of scope
–	not applicable
r	required, dynamically mandatory
x	excluded, dynamically prohibited

5 Conformance

This part of MIL-STD 2045-18500 states requirements for implementations to achieve interworking. A claim of conformance to this part of MIL-STD 2045-18500 is a claim that all requirements in the relevant base standards are satisfied, and that all requirements in the following clauses and in annex A of this part of MIL-STD 2045-18500 are satisfied. Annex A states the relationship between these requirements and those of the base standards.

5.1 Conformance statement

For each implementation claiming conformance to profile AMHx4(D) as specified in this part of MIL-STD 2045-18500, a DSPICS shall be made available stating support or non-support of each option identified in this part of MIL-STD 2045-18500.

The scope of conformance to AMHx4(D) covers MSs and MS-users (UAs). A claim of conformance to profile AMHx4(D) shall confirm that the implementation supports profile AMH13(D) as specified in MIL-STD 2045-17501, Part 5, and shall state whether the implementation supports MS or MS-user functionality.

5.2 MHS conformance

This part of MIL-STD 2045-18500 specifies implementation options or selections that will satisfy the conformance requirements of ISO/IEC 10021 and the CCITT X.400 Recommendations.

Implementations conforming to profile AMHx4(D) as specified in this part of MIL-STD 2045-18500 shall implement the mandatory support (m) features identified as basic requirements in annex A and shall state which optional support (o) features are implemented. They also shall support corresponding MHS EoS and their associated procedures as specified in MIL-STD 2045-18500, Part 1, as appropriate to the scope of this profile and to the role (MS or MS-user) for which conformance is claimed.

Implementations conforming to profile AMHx4(D) as specified in this part of MIL-STD 2045-18500 shall state whether they support any of the optional functional groups specified in MIL-STD 2045-18500, Part 1, apply to the scope of this profile and to the role (MS or MS-user) for which conformance is claimed. For each functional group for which support is claimed, an implementation shall implement all the mandatory support (m) features identified for that functional group in annex A. They also shall support corresponding MHS EoS and associated procedures as specified in MIL-STD 2045-17501, Part 1, as appropriate to the scope of this profile and to the role (MS or MS-user) for which conformance is claimed.

Implementations conforming to profile AMHx4(D) as specified in this part of MIL-STD 2045-18500 shall state the P7 application context(s) for which conformance is claimed.

5.3 Underlying layers conformance

Implementations conforming to profile AMH13(D) as specified in this part of MIL-STD 2045-18500 also shall conform to MIL-STD 2045-17501, Part 5, in accordance with the P7 application context(s) for which conformance is claimed.

Annex A

(normative)

Protocol Requirements List

In the event of a discrepancy between the body of this part of 2045-18500 and the tables in this annex, this annex is to take precedence.

This annex specifies the support what shall or may appear in the implementation columns of a DSPICS. Such requirements are in addition to those specified in annex A of ISO/IEC 10611-5 (reference numbers correspond to items in that annex).

Clause A.1 specifies the basic requirements for conformance to profile AMH13(D). Clause A.2 specifies additional requirements for conformance of optional functional groups.

In each table, the "Profile" column reflects the level of support required for conformance to this DSP (using the classification and notation defined in 3.2). The supplier of an implementation for that claims to conform to profile AMHx4(D) should complete the Support column of the tables in annex A of MIL-STD 2045-18500, Part 5, in accordance with those requirements and any additional requirements in this annex for the type of implementation (MTA or MTS-user) in question.

A.1 Basic requirements

A.1.1 Type of implementation

No additional requirements.

A.1.2 Supported application contexts

No additional requirements.

A.1.3 Supported operations

No additional requirements.

A.1.4 Operation arguments/results

No additional requirements.

A.1.5 MessageSubmissionEnvelope

No additional requirements.

A.1.6 ProbeSubmissionEnvelope

Probes are prohibited in this profile as specified in this part of MIL-STD 2045-18500, Part 5.

A.1.7 AutoForwardRegistrationParameter

No additional requirements.

A.1.8 AutoAlertRegistrationParameter

No additional requirements.

A.1.9 Common data types

No additional requirements.

A.1.10 Extension data types

No additional requirements.

A.1.11 O/R names

No additional requirements.

A.1.12 General Attributes

No additional requirements.

A.1.13 MSP-specific Attributes

Table A.1 MSP-specific Attributes

Ref	Attribute	Profile		Notes/References
		UA	MS	
1	contentDescription	m	m	
2	enacapsulatedContent	o	o	
3	forwardedSignatureData	o	o	
4	mlControlInformation	o	o	
5	mspSequenceSignatureAlgorithm	o	o	
6	mspSequenceSignatureCertificate	o	o	
7	originatorSecurityData	o	o	
8	recipientSecurityData	o	o	
9	signatureBlock	o	o	
10	tUPackage	o	o	

A.2 Optional Functional Groups

There are no additional requirements on optional functional groups in this part of MIL-STD 2045-18500.

A.2.3 Prohibited functional groups

There are no additional requirements on prohibited functional groups in this part of MIL-STD 2045-18500.

Annex B

(normative)

Amendments and corrigenda

International Standards are subject to constant review and revision by the ISO/IEC Technical Committees concerned. The following amendments and corrigenda are approved by ISO/IEC JTC1 and are considered normative references in this part of MIL-STD 2045-18500.

NOTE - Corresponding corrigenda to the equivalent CCITT Recommendations are contained in the joint CCITT/ISO MHS Implementor's Guide Version 8.

MOTIS

ISO/IEC 10021-1/Cor.1:1991
ISO/IEC 10021-1/Cor.2:1991
ISO/IEC 10021-1/Cor.3:1992
ISO/IEC 10021-1/Cor.4:1992
ISO/IEC 10021-1/Cor.5:1992
ISO/IEC 10021-2/Cor.1:1991
ISO/IEC 10021-2/Cor.2:1991
ISO/IEC 10021-2/Cor.3:1992
ISO/IEC 10021-2/Cor.4:1992
ISO/IEC 10021-4/Cor.1:1991
ISO/IEC 10021-4/Cor.2:1991
ISO/IEC 10021-4/Cor.3:1992
ISO/IEC 10021-4/Cor.4:1992
ISO/IEC 10021-4/Cor.5:1992
ISO/IEC 10021-5/Cor.1:1991
ISO/IEC 10021-5/Cor.2:1991
ISO/IEC 10021-5/Cor.3:1992
ISO/IEC 10021-5/Cor.4:1992
ISO/IEC 10021-5/Cor.5:1992

ISO/IEC 10021-6/Cor.1:1991
ISO/IEC 10021-6/Cor.2:1991
ISO/IEC 10021-6/Cor.3:1992
ISO/IEC 10021-6/Cor.4:1992
ISO/IEC 10021-6/Cor.4:1992